SIMON FRASER UNIVERSITY
Senate Committee for Undergraduate Studies
NEW COURSE PROPOSAL

Course Number: CMPT 404-3

Course Title: Cryptography and Cryptographic Protocols
Short Course Title: Cryptography and Protocols

Course vector: 3 lecture

Course Description (for Calendar). Attach a course outline to this proposal.

The main cryptographic tools and primitives, their use in cryptographic applications; security and weaknesses of the current protocols. The notion of security, standard encryption schemes, digital signatures, zero-knowledge, selected other topics.

Prerequisite: MACM 201. CMPT 307 and 308 are recommended.

Corequisite: none

Course(s) to be dropped if this course is approved: none

Rationale for Introduction of this Course:

With the development of the Internet and electronic commerce, computer security has become extremely important. Although a cryptography course was offered by the School of Computing Science several years ago, at the moment there is no course with a fixed curriculum in this area. The proposed course covers cryptographic primitives, protocols, and their implementations, a significant component of computer security. It will provide students with understanding the principles and techniques of cryptography. It will also be a complement to the existing MACM 442 course that mostly concentrates on number theoretic cryptographic primitives.

This course has previously been offered as CMPT 409 (Special Topics)

Scheduling and Registration Information:

Indicate effective **semester/year** course would be first offered and planned **frequency** of offering thereafter.

Annually starting in fall 2008 on the Burnaby campus. This course will be offered at the Surrey and downtown campuses as demand and instructional resources allow.

Waiver required: no

Will this be a required or elective course in the curriculum?

Elective.

What is the probable enrolment when offered?

15-25 students

Which of your present CFL faculty have the expertise to offer this course?

Andrei Bulatov, Valentine Kabanets, Gabor Tardos

Are there any proposed student fees associated with this course other than tuition fees? (if so, attach mandatory supplementary fee approval form)

no

Resource Implications:

Note: Senate has approved (S.93-11) that no new course should be approved by Senate until funding has been committed for necessary library materials. Each new course proposal must be accompanied by a library report and, if appropriate, confirmation that funding arrangements have been addressed.

Campus where course will be taught:

Burnaby; Surrey and downtown if demand exists.

Library report status ____

Provide details on how existing instructional resources will be redistributed to accommodate this new course. For instance, will another course be eliminated or will the frequency of offering of other courses be reduced; are there changes in pedagogical style or class sizes that allow for this additional course offering?

This course has previously been offered as a special topics course. It is expected that offerings of this course will replace offerings of lower-demand courses.

Any outstanding resource issues to be addressed prior to implementation: space, laboratory equipment, etc.

none

Approvals

1. **Departmental approval** indicates that the Department has approved the content of the course, and has consulted with other Departments and Faculties regarding proposed course content and overlap issues.

____

Chair, Dept./School Date

____

Chair, Faculty Curriculum Committee Date

2. **Faculty approval** indicates that all the necessary course content and overlap concerns have been resolved, and that the Faculty/Department commits to providing the required Library funds.

______________________________ Date: ____________________

Dean or Designate

List which other Departments and Faculties have been consulted regarding the proposed course content including overlap issues. *Attach documentary evidence of responses.*

____

____

____

____

Other Faculties approval indicates that the Dean(s) or designate of other Faculties affected by the proposed new course support(s) the approval of the new course.

________________________________ Date: ______________________

________________________________ Date: ______________________

3. SCUS approval indicates that the course has been approved for implementation subject, where appropriate, to financial issues being addressed.

Course approved by SCUS (Chair of SCUS)

________________________________ Date: ______________________

Approval is signified by date and appropriate signature.

Proposed CMPT 404 Course Outline

OBJECTIVE/DESCRIPTION:

The course focuses on foundations of modern cryptography. It rigorously defines the basic requirements to cryptographic schemes, privacy and authenticity. It introduces required constructions and results from complexity theory, and shows how these results are used to built provably secure cryptographic schemes. We also consider how these principles are used in the existing systems, and see why many of the widely used schemes such as SSL and SSH may be insecure.

TOPICS:

o Basics of probability, cryptography, and complexity. Historical remarks
o Concepts of privacy and authenticity: perfect, statistical, and computational
o Pseudo-random generators and functions
o One-way functions
o Private-key encryption: constructions
o Private-key encryption in practice: block ciphers
o Trapdoor functions and public-key encryption
o Message authentication, digital signatures, and hashing
o Zero-knowledge proofs
o Survey of the cryptographic components of the existing protocols

GRADING:

`4 assignments (12.5% each), course project (50%)`

TEXTBOOKS:

o Oded Goldreich. Foundations of cryptography,
Cambridge Univ.\ Press, 2001,2004

o Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone.
Handbook of Applied Cryptography.